学内ローミングおよび国際ローミングに対応した情報科学研究科・新無線LANシステムの構築について

学内ローミングおよび国際ローミングに対応した情報科学研究科・新無線 LAN システムの構築について

後藤英昭
東北大学サイバーサイエンスセンター / 情報科学研究科 (兼務)

1 はじめに

2003 年の TAINS ニュース No.30 [1]、および 2005 年の TAINS ニュース No.33 [2] において、情報科学研究科における無線 LAN システムの運用について紹介しました。2008 年 3 月の教育用計算機システムの更新に伴い、館内の無線 LAN システムも一新されましたので、その概要を紹介します。

2 複数認証方式とローミングに対応する無線 LAN システム

2.1 ユーザ認証方式の推移

2003 年の初代システムでは、ユーザ認証の仕組みとして Secure Shell 認証方式を採用しました [1]。当時は、無線 LAN システムのユーザ認証機構として企業向けのものが幾つかある程度で、一般ユーザ向けの公衆無線 LAN で利用できるような、手頃で安全なものはありませんでした。このような背景から、筆者らは Secure Shell 認証方式を開発し [3]、当時のシステムに応用しました。この方式は、これまでに他大学等でも利用実績があります。

大学に無線 LAN システムが普及するにつれて、大きな大学では特に、異なる部局にまたがる相互利用の必要性が認識されるようになりました。筆者らは学内における無線 LAN ローミングを実現する方法として、VPN(Virtual Private Network) 技術を応用した「どこでも TAINS」方式を開発し、学内ネットワーク TAINS で利用促進活動を行いました。情報科学研究科の無線 LAN システムもこれに対応すべく、2005 年に機能拡張を行いました [2]。

近年では、ホテルや空港、駅、カフェ、あるいは道路における公衆無線 LAN サービスが普及し、ウェブ認証や IEEE802.1X 認証といった手法が広く使われるようになってきました。教育研究機関向けの国際的な無線 LAN ローミング基盤も立ち上がり、欧州の TERENA で開発された「eduroam (エデュローム)」[4] というシステムに東北大学も 2006 年に接続しました [5]。また、マルチ SSID 対応の無線アクセスポイントの価格低下と普及により、複数認証方式の実現も容易になってきました。

2.2　サポートする認証方式

新システムでは、無線アクセスポイントのマルチ SSID 機能を利用して、次の三種類の認証方式を同時サポートすることにしました。

- 「どこでも TAINS」方式 (VPN 認証方式、学内ローミング用)
- 「eduroam」方式 (国際無線 LAN ローミング)
- 「ウェブ認証」方式

情報科学研究科では、他の建物やキャンパスに居住する教員・学生が多いという事情により、ローミングへの対応が欠かせません。大は小を兼ねるという意味では「eduroam」だけでも十分に見えるのですが、利便性を考えると問題があります。「eduroam」では IEEE802.1X による認証 (以下 1X 認証と呼ぶ) が標準ですが、1X 認証では端末にインストールするドライバ (サプリンカントと呼ばれる) と無線 LAN ドライバ、無線アクセスポイント、認証情報をやりとりする RADIUS サーバの間に不整合や不具合が根強く残っており、まだ安定しているとは言い難い状況です。端末を利用するサイトが変わると、ネットワーク接続の際に認証に失敗したり、しばしばトラブルに見舞われることが経験的に知られています。また、学内でローミングを実現するには、他部局でも RADIUS サーバが整備される必要があります。このため、長年の利用実績があり、安定した環境が提供できる「どこでも TAINS」を第一の認証方式として採用しました。

「どこでも TAINS」方式では、端末側に PPTP や OpenVPN の VPN クライアントプログラムがあれば良く、特に PPTP 用のクライアントプログラムは MS-Windows XP/Vista、MacOS X、その他幾つかの PDA 等に標準的に組み込まれています。利用者は事前に特殊なプログラムをインストールしておく必要がなく、この点でシステムの利便性は非常に高いと言えます。

一方「どこでも TAINS」には、学外のローミングに対応できないという制約があります。訪問者のネットワーク利用の便宜をはかるために、国内でも新しい試みである「eduroam」にいち早く対応することにしました。また、情報科学研究科に無線 LAN のアカウントを作成することで、研究科の教職員や学生が国内外の eduroam 加盟機関でネットワーク利用が可能になるというメリットも生じます。

現在、「eduroam」には欧州で約 30 ヶ国、アジア太平洋地域ではオーストラリア、香港、台湾、日本、中国が加盟しており、他の一部の国でも導入準備中です。カナダでも幾つかの大学で利用が始まったようです。

第三の方式の「ウェブ認証」は、他の二方式が利用できない場合の非常手段という位置付けで導入しています。この方式は、また、訪問者向けに一時的に無線 LAN サービスを提供するのに便利でしょう。

「ウェブ認証」は公衆無線 LAN サービスなどでも一般的で、ウェブブラウザを開くだけで ID/パスワードの入力画面が表示されるなど、利用者にとって馴染みやすいものです。しかしながら、端末が偽のアクセスポイントを介して偽の認証ページに誘導されるなど、悪意のあるユーザ

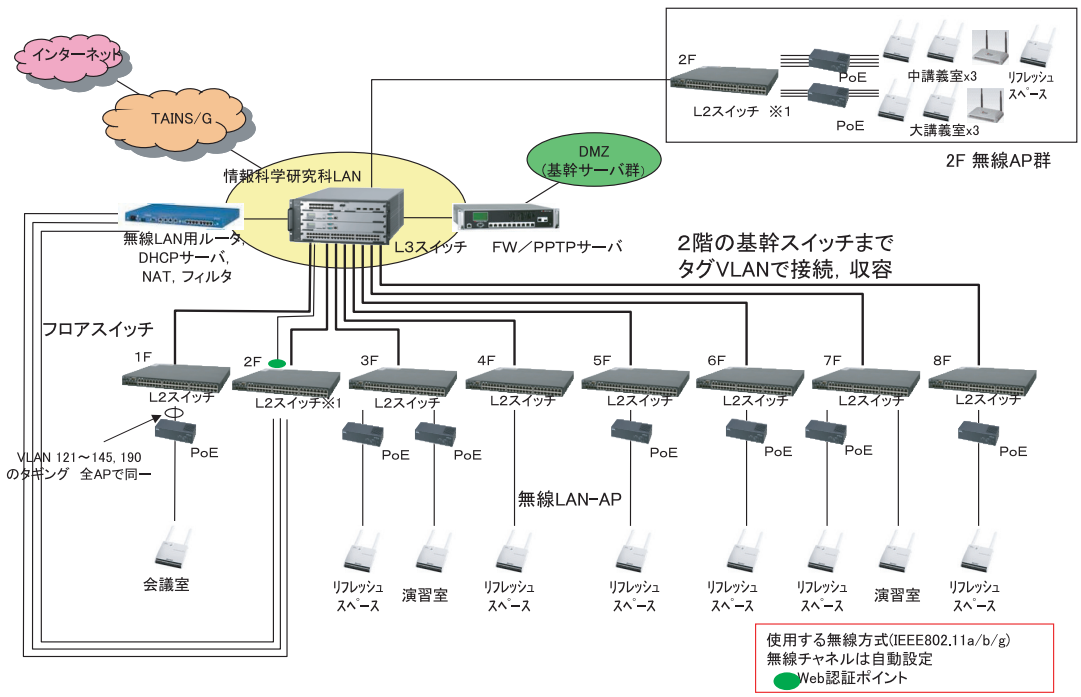

図 1: 情報科学研究科無線 LAN システム構成図 (NEC ソフトウェア東北様より提供)

に ID/パスワードを盗まれる危険性が高いというセキュリティ上の問題があります。SSL 対応の認証ページを用いることで、若干のセキュリティ向上策にはなりますが、そもそも多くの利用者がブラウザの http と https の表示の差にあまり気を配らない現状では、偽のページに誘導されても気付きにくいと言えます。VPN 方式や 1X 認証では、端末側の設定を一度正しく行っておけば、基本的にはユーザ認証時に偽のサーバに対して ID/パスワードを通知してしまう可能性はほとんどありません。一方、「ウェブ認証」ではユーザ認証が行われるたびに、利用者の不注意によって ID/パスワードを漏洩する危険性が生じます。

2.3 システム構成

無線 LAN システムの構成図を図 1 に示します。

無線アクセスポイントは二種類あり、タイプ A が 14 台、タイプ B が 2 台の計 16 台です。従来システムで講義室とリフレッシュスペースに設置されていたアクセスポイントを新製品に置き換えたのに加えて、要望の多かった会議室 (一階) と一部の演習室に新規にアクセスポイントを設置しました。アクセスポイントの写真を図 2, 3 に示します。すべてのアクセスポイントが 11b/a/g の無線規格に対応しています。

それぞれのアクセスポイントでは、マルチ SSID の機能を有効にして、前述の三種類の認証方式に対応した SSID を付与しています。具体的には、タイプ A のアクセスポイントにおいて、

図 2: リフレッシュスペースの無線 AP

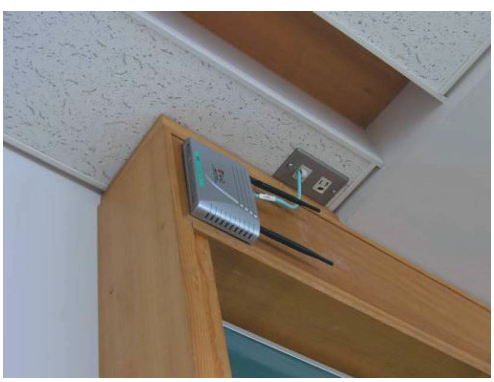

図 3: 講義室の無線 AP (タイプ B)

「どこでも TAINS」の SSID が “tains-xF” (x は階番号)、「eduroam」が “eduroam”、「ウェブ認証」が “gsis” に設定されています。

大変残念なことに、調達によって導入されたタイプ A の機種では、製品の仕様により SSID が一つしかブロードキャストできないことが判っています[*1]。SSID がブロードキャストされていない (ビーコンが出ていない) 場合、利用者が事前に SSID を端末に登録しておかないとアクセスポイントに接続できず、無線 LAN のドライバによっては SSID が登録されていても接続できないという問題が生じることがあります。このため、企業での利用では大きな問題にならなくても、キャンパス無線 LAN や公衆無線 LAN では、SSID がブロードキャストされていないことは利便性の大幅な低下を招きます。また、当該モデルでは、二個目以降の SSID について暗号化を無効にできない、利用できる認証方式に制約があるなどの問題も知られています。

そのため、やむを得ず、以下の方針でタイプ A のアクセスポイントを運用することにしました。

[*1] 今回、私は調達に関わっておらず、当該モデルの納入を回避することができませんでした。納入業者に非はありません。

- 学内で利用頻度が高い「どこでも TAINS」は、暗号化や WEP を使えないので、プライマリの SSID とする。SSID はブロードキャストする。
- 「eduroam」は標準的な SSID として “eduroam” が広く知られているので、端末側に SSID が設定されていることを期待する。
- 「ウェブ認証」では利便性の観点から暗号化や WEP を使わない運用が望ましいが、利用頻度が低いとみなし、SSID “gsis” と共通の WEP キーを公開する。

しかし、SSID が見えない状態で接続に失敗する端末が無視できないことから、需要が多い講義室については、タイプ B のアクセスポイント (アライドテレシス AT-TQ2403) を別途導入・設置して、「eduroam」と「ウェブ認証」の SSID もブロードキャストできるようにしました。タイプ A との混同を避けるために、SSID はそれぞれ “eduroam2”、“gsis2” に設定されています。

マルチ SSID では、SSID ごとに異なるタグの付いた VLAN がアクセスポイントから出てきます。すなわち、タイプ A では三種類のタグが付いた VLAN が一つの tagged port から出てきます。このタグ付きのネットワークを各フロアにあるスイッチに収容し、タグをばらさないで二階の基幹スイッチまで引いています。

VLAN は二階のスイッチでタグを外され、それぞれの認証方式に対応したゲートウェイや認証スイッチに送られます。無線 LAN 用ルータにおいて、「どこでも TAINS」や「eduroam」で必要なフィルタリングを施し、DHCP による端末へのアドレス付与や、アドレス変換 (NAT) を行っています。「どこでも TAINS」のフィルタリングに関しては、文献 [6] を参照して下さい。「eduroam」に関しては VPN-only ポリシを採用しており、主要な VPN プロトコルのみを通すようなフィルタが適用されています [5]。

「ウェブ認証」の機能は、市販の認証機能付きのスイッチ (認証スイッチ) を用いて実現しています。少しでもセキュリティを高められるように、認証画面では SSL を使うようになっています。スイッチには、国立情報学研究所と 7 大学の情報基盤センター群による UPKI 構築事業で提供されているサーバ電子証明書 [7] を導入し、標準的なブラウザで警告が出ないようにしています。これにより、予めブラウザに証明書を登録する必要がなくなるとともに、初回のログインにおいて利用者が偽のサーバから偽の証明書を掴まされる危険性が低くなります。

当システムには、「どこでも TAINS」や学外から使えるような VPN(PPTP) サーバも含まれます。VPN サーバ用のアカウントは、基幹サーバ群と連携するような構成になっています。「eduroam」と「ウェブ認証」で利用する RADIUS サーバも、アカウントを共用しています。すなわち、基幹サーバにアカウントを作成すれば、世界中の eduroam 対応サイトでネットワーク接続が可能になります。なお、UNIX 系のアカウントと RADIUS 用のアカウントの同期が難しいのと、システムとネットワークではログインのセキュリティレベルが大きく異なることに配慮して、無線 LAN/VPN 用のアカウントは UNIX 系と別に作成するようになっています。

3　おわりに

本稿では、学内の無線 LAN ローミング「どこでも TAINS」および国際無線 LAN ローミング基盤「eduroam」に対応した、情報科学研究科棟の新無線 LAN システムを紹介しました。

今回構築したシステムでは、館内ネットワークのスイッチのタグ VLAN 機能を利用することによって、階をまたがる無線 LAN 専用の線を省略し、導入コストが低くなっています。また、このネットワーク構成には、アクセスポイントのマルチ SSID 機能を使っても、物理線をほとんど増やさずに済むという利点もあります。より大規模なシステムでは統合型の無線 LAN 製品を利用すべきでしょうが、小規模なシステムでは本稿で紹介したような構成でも十分だろうと思います。

これから無線 LAN システムを整備する部局においては、ぜひローミング対応のシステムを構築することをお奨めします。

謝辞

当無線 LAN システムの構築にあたっては、以下の方々にご協力をいただきました。紙面を借りてお礼申し上げます。

NEC ソフトウェア東北株式会社 第一ソリューション事業部　佐藤 佳彦 様
NEC ソフトウェア東北株式会社 第一ソリューション事業部　高橋 昭 様
NEC ソフトウェア東北株式会社 第一ソリューション事業部　山本 英樹 様

参考文献

[1] 後藤英昭, “情報科学研究科における無線 LAN システムの運用について,” TAINS ニュース, No.30, pp.16–26, 2003.
(http://www.tains.tohoku.ac.jp/news/news-30/1626.html)

[2] 後藤英昭, “情報科学研究科における無線 LAN システムの運用について (2) — 「どこでも TAINS」への対応,” TAINS ニュース, No.33, pp.10–14, 2005.
(http://www.tains.tohoku.ac.jp/news/news-33/1014.html)

[3] authipgate – Simple Authenticating Gateway for Linux. http://freshmeat.net/projects/authipgate/

[4] L. Florio and K. Wierenga, “Eduroam, providing mobility for roaming users,” Proc. 11th International Conference EUNIS2005, 2005.

[5] 後藤英昭, “eduroam の構築と参加方法,” グリッド・UPKI 活用のための CSI 講演会 講演予稿集, pp.31-42, 2007.10.12.

[6] 後藤英昭, 水木敬明, 曽根秀昭, “無線・有線 LAN ローミングシステム「どこでも TAINS 2」,” TAINS ニュース, No.35, pp.5-7, 2008.
(http://www.tains.tohoku.ac.jp/news/news-35/0507.html)

[7] 澤田勝己, 曽根秀昭, “東北大学におけるサーバ証明書発行の試行運用についての報告,” 大規模科学計算システム広報 SENAC Vol.41, No.1, pp.45-51, 2008.
(http://www.cc.tohoku.ac.jp/refer/pdf_data/v41-1p45-51.pdf)